DOCUMENT RESUME

ED 467 385 JC 020 558

AUTHOR	Campbell, Robert D.; Hawthorne, Elizabeth K.
TITLE	Cybersecurity Education in Community Colleges across America: A Survey of Four Approaches by Five Institutions.
PUB DATE	2002-00-00
NOTE	12p.
PUB TYPE	Reports - Descriptive (141)
EDRS PRICE	EDRS Price MF01/PC01 Plus Postage.
DESCRIPTORS	College Programs; *Community Colleges; *Computer Security; Educational Innovation; *Educational Technology; *Internet; *Technical Education; Two Year Colleges
IDENTIFIERS	Community College of the Air Force Al; Community College of the Air Force TX; Edmonds Community College WA; Northern Virginia Community College; Roane State Community College TN; Seminole Community College FL

ABSTRACT

This document describes four distinct approaches to education in the area of cybersecurity currently taught at community colleges across America. The four broad categories of instruction are: (1) degree program--four semesters of study leading to an associate's degree; (2) certificate program--two semesters leading to an institution-conferred certificate; (3) credit course that is part of an existing program of study; and (4) non-credit program of preparation for an industry certification. The authors profiled the cybersecurity community college degree program at Seminole Community College (Florida) and described the content of the curriculum as a career education degree that requires 63 semester-hour credits covering the concepts of security analysis, security policy, troubleshooting security. Two certificate programs, one at Seminole and one at Northern Virginia Community College, are briefly described, including details of their program expectations and curriculum content. The Community College of the Air Force (Texas) and Northern Virginia Community College were the only institutions identified as offering cybersecurity courses as part of already established programs of study (Information Systems Technology and Administration of Justice respectively). Finally, the authors profile the non-credit industry certification programs offered at Edmonds Community College (Washington) and Roane State Community College (Tennessee). (RC)

Reproductions supplied by EDRS are the best that can be made
from the original document.

Cybersecurity Education in Community Colleges Across America:

A Survey of Four Approaches by Five Institutions

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
This document has been reproduced as received from the person or organization originating it.
Minor changes have been made to improve reproduction quality.
Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

by

Robert D. Campbell (Rock Valley College)
and
Elizabeth K. Hawthorne (Union County College)

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY

R. Campbell

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

ED 467 385

Introduction

Since September 11, 2001, Americans are more aware of threats to computer system vulnerabilities and the urgent need to educate the workforce quickly and effectively. Education in "cybersecurity" and information assurance falls into two distinct categories. The first is training, marked by an emphasis on particular systems, situations, or environments rather than broad principles. The second is scholarly, marked by an emphasis on underlying principles, concepts, and their applications. Scholarly education and training complement one another.

This paper describes four distinct approaches to education in the area of cybersecurity currently being taught at community colleges across America. We define four prototypical avenues for packaging the instruction, as are commonly found in the two-year college environment, and describe the offerings at each institution. We will describe these instantiations in sufficient detail to provide insights into the efforts currently underway and to serve as a point of departure for other community colleges interested in offering education in cybersecurity.

The four broad categories of instruction are:

- A four-semester program of study leading to an associate degree (hereafter referred to as the Degree Program);
- A two-semester program of study leading to an institution-conferred certificate (hereafter referred to as the Certificate Program);
- A credit course that is part of an existing program of study (hereafter referred to as the Course);
- A non-credit program of preparation for an industry certification (hereafter referred to as the Credential Program).

The Degree Program we describe is intended to prepare students for immediate employment in the field of computing with special emphasis on careers related to the area of cybersecurity and its associated fields. The Certificate Program we describe is intended to provide an abbreviated program of study to augment the institution's degree programs and to provide students the opportunity to obtain specialized training in cybersecurity. The Course we describe is intended as either an elective or required component in a program of study otherwise not specifically focused on cybersecurity,

TC 020558

BEST COPY AVAILABLE

providing students an introduction to these topics. The Credential Program we describe is intended to specifically prepare students to sit for a targeted industry certification exam in cybersecurity and is not necessarily related to credit-program offerings.

These four approaches to cybersecurity education are generally available to all comprehensive community colleges, and are familiar categories to faculty and administrators in this sector of higher education. This paper, then, demonstrates that some two-year colleges in the United States have already availed themselves of these avenues in addressing the field of cybersecurity. Other community colleges may be poised to do likewise, once model implementations are publicized and the skill sets for this area of instruction are better identified. It is our hope that this paper will foster and promote those efforts.

Degree Program

This paper classifies a degree program as a four-semester program of study leading to an associate degree. To date, we located one community college that offers such a degree program. Seminole Community College (SCC) in Florida offers an "e-Business Technology Security Specialization" Associate of Science (A.S.) degree. An A.S. degree in the Florida community college system is typically described as a career education degree, equivalent to the A.A.S. degree in many other states. In the words of SCC, "A.S. programs provide [students] with the knowledge necessary to perform and excel in a particular profession. Some of the credits earned in an A.S. degree program can be transferred to a four-year college or university ... however, the A.S. curriculum is not considered equal to the first two years of a bachelors degree."

Seminole Community College (http://www.seminole.cc.fl.us) describes this program as preparing graduates for career opportunities in fields such as Internet and network security specialist, Internet technical support specialist, Internet and network security technician, and Database security technician. In the program narrative, SCC states that the program focuses on the security aspects of Internet commerce over multiple systems (Internet, intranet, and local systems), providing security skills for an e-business environment in the areas of security analysis, designing and creating a security system, troubleshooting security, testing security measures, and creating, implementing, and maintaining a security policy, as well as additional consideration given to legal and ethical issues, current and emerging legislation, virus threats, accounts and groups, file systems, and network security.

The SCC degree program consists of a total of 63 semester-hour credits, made up of 30 credits in "major courses", 12 credits in "support courses", 6 credits in "electives" and 15 credits in "general education". This distribution is detailed in the table below.

Major Course		
Course#	**Course Name**	**Credits**
APA 1111C ACG 2021C	Office Systems Accounting I **or** Principles of Financial Accounting **(choose one)**	3
CET 1652C	Computer Network Architecture	3
CGS 2069	Survey of e-Business Technology	3
CGS 2100C	Microcomputer Software Packages	3
COP 2066	Internet Web Essentials	3
GEB 1011 GEB 1136	Introduction to Business **or** Foundations of e-Business **(choose one)**	3
GEB 2442	e-Business Law and Ethics	3
MAN 2021 MAN 2800	Introduction to Management **or** Small Business Management **(choose one)**	3
MAN 2581	Project Management	3
MAR 2011	Marketing	3
	Total:	**30**
Support Courses		
CEN 1543	Introduction to Internetworking Security	3
CEN 2525	Advanced Internetworking Security	3
CET 2665C	Firewall Configuration and Management	3
CET 2760C	Web Server Management	3
	Total:	**12**
Electives: choose two from the list below		
CET 2662C	Security Testing and Auditing	3
CET 2664C	Encryption and Cryptography	3
CET 2666C	Configuring IP Security	3
	Total:	**6**
General Education Courses		
ENC1101	English I	3
SPC1600	Introduction to Oral Communication	3
HUM xxxx	Humanities General Education Elective	3
xxx xxxx	Mathematics General Education Elective	3
xxx xxxx	Social Science General Education Elective	3
	Total:	**15**
	Degree Total:	**63**

The following overviews provide insight into the contents of each of the major courses, support courses, and electives.

Major Courses

- **APA 1111C - Office Systems Accounting I** … focuses on fundamental financial record keeping and reporting using computers and general ledger software to automate record keeping activities.
- **ACG 2021C - Principles of Financial Accounting** … introduces students to preparing financial statements for partnerships and corporations.
- **CET 1652C - Computer Network Architecture** … introduces the principles and methods behind Local Area Networks and Internet/web connectivity. (Prerequisite: CGS 2069- Survey of e-Business or CET 1486C - Network Concepts and Operating Systems)
- **CGS 2069 - Survey of e-Business Technology** … focuses on communications, network concepts, Internet, World Wide Web, and e-Commerce fundamentals.
- **CGS 2100C - Microcomputer Software Packages** … introduces students to major application software packages using Microsoft Office.
- **COP 2066 - Internet Web Essentials** … includes use of web browsers to access Internet services, creation of simple web pages, concepts related to WWW, Internet, e-Mail, Telnet, Gopher, security measures, and FTP; non-technical topics include legal, ethical, and privacy issues, and etiquette. (Prerequisites: CGS 2100C - Microcomputer Fundamentals and Business Applications; CGS 2069 - Survey of e-Business or CET 1486C - Network Concepts and Operating Systems)
- **GEB 1136 - Foundations of e-Business** … provides a functional and general view of e-Business and e-Commerce management strategies, Business-to-Business (B2B), Business-to-Consumer (B2C), and Intra-Business models.
- **GEB 2442 - e-Business Law and Ethics** … provides an overview of web-based business legal issues, and intellectual property rights including patents, copyrights, trademarks, and trade secrets.
- **MAN 2021 - Introduction to Management** … studies the essentials (planning, organizing, staffing, directing, controlling) of operational management in a business environment
- **MAN 2800 - Small Business Management** … presents a fundamental approach to managing a small firm and the necessary steps in planning and evaluating small business concerns.
- **MAN 2581 - Project Management** … covers the concepts (plan, organize, implement) of project management for information technology using real-world examples.
- **MAR 2011 – Marketing** … introduces the marketing process: consumer behavior, product planning, marketing institutions and functions, and promotional and pricing strategies.

Support Courses

- **CEN 1543C - Introduction to Internetworking Security** … examines the principles, mechanisms, and implementations of network security and data protection, company-wide security process and performing a security audit; controlling access to systems, resources, and data, and security issues of common operating systems. (Prerequisite: CET 1652C - Computer Network Architecture)
- **CEN 2525 - Advanced Internetworking Security** … examines in greater depth the principles, mechanisms, and implementation of network security and data protection. (Prerequisite: CEN 1543 - Introduction to Internetworking Security)
- **CET 2665C - Firewall Configuration and Management** … examines how firewalls are used as a network security solution, network address translation, proxy servers, inspection firewalls, basic VPNs, and intrusion detection systems; emphasis on installing, configuring, and managing today's most popular software and hardware firewalls.
- **CET 2760C - Web Server Management** … prepares students to setup, configure, and manage a complete web server; fundamental Web server security and other Web server-related issues. (Prerequisites: CET 1515C - Web Authoring, CET 1492C - NetWare Administration)

Electives

- **CET 2662C - Security Testing and Auditing** … focuses on establishment and use of testing and auditing policies; installation, configuration, and use of related software tools
- **CET 2664C - Encryption and Cryptography** … introduces basic theories and practices of cryptographic techniques for computer security; encryption (secret-key and public-key), digital signatures, secure authentication, e-Commerce (anonymous cash, micro payments), key management, cryptographic hashing, and Internet voting systems. (Prerequisite: CEN 1543C - Introduction to Internetworking Security)
- **CET 2666C - Configuring IP Security** … focuses on advanced IP security configurations, evaluation of different protocols used to provide network services, identifying vulnerabilities in commonly used Internet service protocols and concepts behind IP security protocol. (Prerequisite: CET 2665C - Firewall Configuration and Management)

Certificate Program

A certificate program is an abbreviated program of study leading to an institution-conferred certificate. This type of study provides students with an existing background in networking the opportunity to further develop specialized skills in cybersecurity. To date, we have located two community colleges that offer such certificate programs. Seminole Community College in Florida offers an "e-Business Security Technical Certificate" that is a subset of the degree program described in the discussion above.

Northern Virginia Community College (NVCC) offers a career studies certificate in "Network Security."

Northern Virginia Community College (http://www.nv.cc.va.us) describes this program as an enhanced competency module to provide expertise in security to networking specialists. This curriculum will prepare networking specialists for employment as network security specialists or Internet security specialists. The NVCC certificate program consists of a total of 28 semester-hour credits. This distribution is detailed in the table below.

Course#	Course Name	Credits
IST 245	Network Security Basics	3
IST 246	Network Attacks, Computer Crime and Hacking	4
IST 247	Network Communication, Security and Authentication	4
IST 293	Studies in Network Security	3
IST 248	Internet/Intranet Firewalls and e-Commerce Security	4
IST 266	Network Security Layers	4
IST 267	Legal Topics in Network Security	3
ENG/SPD	Elective	3
	Total:	**28**

The following overviews provide insight into the contents of each of the courses.

IST 245 Network Security Basics ... explores the basics of network security in depth, including security objectives, security architecture, security models and security layers; the topics of risk management, network security policy, and security training; and the five security keys: Confidentiality, Integrity, Availability, Accountability, and Auditability. (Prerequisite: an AAS degree or higher in a Networking field)

IST 246 Network Attacks, Computer Crime and Hacking ... provides an in-depth exploration of various methods for attacking and defending a network; network security concepts from the point of view of hackers and attack methodologies, Intrusion Detection Systems (IDS), malicious code, computer crime, and industrial espionage. (Prerequisite: an AAS degree or higher in a Networking field.)

IST 247 Network Communication, Security and Authentication ... provides an in-depth exploration of various communication protocols from the point of view of the hacker in order to highlight protocol weaknesses, with a concentration on TCP/IP; includes topics of Internet architecture, routing, addressing, topology, fragmentation, and protocol analysis; use of various utilities to explore TCP/IP. (Prerequisite: an AAS degree or higher in a Networking field)

IST 248 Internet/Intranet Firewalls and e-Commerce Security .... provides an in-depth exploration of firewall concepts, types, topology, and the firewall's relationship to

the TCP/IP protocol; client/server architecture, the web server, HTML, and HTTP in relation to web security and e-commerce security; digital certification, X.509, and Public Key Infrastructure (PKI). (Prerequisite: an AAS degree or higher in a Networking field)

IST 266 Network Security Layers ... provides in-depth exploration of security layers needed to protect the network; physical security, personnel security, operating system security, software security and database security. (Prerequisite: an AAS degree or higher in a Networking field and successful completion of the Network Security Career Studies Certificate first semester)

IST 267 Legal Topics in Network Security ...provides an in-depth exploration of the civil and common law issues that apply to network security; statutes, jurisdictional and constitutional issues related to computer crime and privacy; rules of evidence, seizure and evidence handling, court presentation and computer privacy. (Prerequisite: an AAS degree or higher in a Networking field and successful completion of the Network Security Career Studies Certificate first semester courses)

IST 293 Studies in Network Security ... provides an opportunity for students in multiple disciplines to discover and discuss a variety of issues related to security concerns in a computer network environment.

Course

This paper refers to course as either a required or elective credit course that is part of an already established program of study. The Community College of the Air Force (CCAF) and Northern Virginia Community College each offer such courses.

The Community College of the Air Force (http://www.au.af.mil/au/ccaf/index.htm) is the largest multi-campus community college in the world with 122 affiliated schools and education service offices servicing 373,000 registrants -- enlisted members pursuing their associate degree. The Community College of the Air Force offers a course titled Computer Systems Security as part of an Information Systems Technology program of study. See the technical core requirements for this program in the table below or visit http://www.au.af.mil/au/ccaf/catalog/2002cat/ter_0iyy.htm for complete program requirements.

CCAF Information Systems Technology (technical core only)

Course Name	***Max Semester Hours***
Airborne Information Systems	24
Broadcast Information Systems/Management	15
CCAF Internship	18
Command and Control Information Systems	15
Communications Networking	12

Communications-Electronics Program Management	12
Computer Systems Security	6
Data Information Systems/Management	20
Personnel Data Systems	12
Telecommunications Administration/Industry Regulation	6
Telecommunications Technology	6

The course overview for the Computer Systems Security course is as follows:

Computer Systems Security ... addresses procedures for administering and monitoring automatic data processing security; security development, policies, duties and responsibilities, system abuse, and establishment of security training programs.

The Community College of the Air Force also offers a course in Informational Security as part of an Information Management program of study. See the technical core requirements in the table below or visit
http://www.au.af.mil/au/ccaf/catalog/2002cat/ter_1auy.htm
for complete program requirements. Unfortunately, a description of the course content was not available.

CCAF Information Management Program (technical core only)

	Max Semester Hours
CCAF Internship	18
Informational Security	3
Information Systems Administration	12
Information Systems Management	9
Microcomputer Software Applications	9
Office Equipment	3
Postal Operations/Management	15
Records/Publications Management	6

Northern Virginia Community College (http://www.nv.cc.va.us) offers two security related courses as part of a certificate or Associate in Applied Science degree in the Administration of Justice program of study. Details regarding this program of study are located at the web address listed above. The NVCC Computer Security course is an elective, while the Information Security course is required for both the certificate credential and A.A.S. degree. The catalog descriptions for these courses are provided below.

ADJ 157 Computer Security … examines security concerns with access controls, shutdown alternatives, hardware and software protection, and data encryption.

ADJ 256 Information Security … studies the means of protecting both government classified and private business information. Surveys techniques of storing, transmitting, destroying, and controlling access to sensitive information.

Credential Program

For the purpose of this discussion, a credential program is a non-credit program of preparation for a specific industry certification. This type of study specifically prepares students to sit for a targeted industry certification examination. Two community colleges, Edmonds Community College (ECC) in Washington and Roane State Community College (RSCC) in Tennessee, offer such preparation for the Security Certified Network Professional and the Security Certified Network Architect professional certifications conducted by Ascendant Learning; details on these credentials can be found at http://www.securitycertified.net/certifications.htm. The program descriptions at both institutions are nearly identical.

Edmonds Community College (http://www.btc.edcc.edu/) describes the Security Certified Program as designed for the IT Professional who wishes to verify his or her skills as a Security Professional. The two credential programs offered by ECC are the SCNP (Security Certified Network Professional) and the SCNA (Security Certified Network Architect).

The ECC SCNP program focuses on two critical areas of security described as the foundational defense of networks: firewalls and intrusion detection. The SCNP program is divided into two courses, the first being Network Security Fundamentals (NSF) and the second being Network Defense and Countermeasures (NDC). The following overviews provide insight into the contents of each of the courses.

Network Security Fundamentals … is a 48-hour course of training consisting of a combination of teacher-led lecture, in-class discussions, and hands-on lab exercises. There are ten domains covered in the course, covering issues such as: Securing Windows, UNIX, and Linux operating Systems, Advanced TCP/IP, Security Fundamentals, Security Implementation, Router Security, and Attack Methods. (*Prerequisites:* Students need to possess one of the following certifications, or have equivalent training/work experience: CCNA, CNA, CNE, CIW Associate, iNet+, MCP, MCSE, NETWORK+)

Network Defense and Countermeasures … is a 40-hour course of training consisting of a combination of teacher-led lecture, in-class discussions, and hands-on lab exercises. There are eight domains covered in the course, covering issues such as: Risk Analysis, Firewalls, Intrusion Detection Systems, Security Policies, and Virtual Private Networks. This course will focus heavily on Firewalls and Intrusion Detection Systems, providing for nearly 70% of the content. (*Prerequisite:* Network Security Fundamentals)

The ECC SCNA program is for those individuals who wish to take their Security Skills to the next level. Students learn how network security is moving towards trusted communication, and how the defensive schemes alone are not enough. Dealing with two critical areas of communication, the SCNA program deals extensively with Public Key Infrastructure (PKI) and Biometrics. At ECC, the SCNA program is divided into two courses: PKI and Biometrics Concepts and Planning; and PKI and Biometrics Implementation.

PKI and Biometrics Concepts and Planning ...is a 40-hour course of training consisting of a combination of teacher-led lecture, in-class discussions, and hands-on lab exercises. There are six domains covered in the course, covering issues such as: Cryptography Fundamentals, Digital Signatures, Biometrics Fundamentals, PKI Fundamentals, PKI Standards, and Strong Authentication. (Prerequisites: Students need to have taken the SCP Security Fundamentals and Network Defense and Countermeasure courses.)

PKI and Biometrics Implementation ...is a 40-hour course of training consisting of a combination of teacher-led lecture, in-class discussions, and hands-on lab exercises. There are six domains covered in the course, covering issues such as: Sign-On Solutions, File Encryption Solutions, Certificate Server Deployment, PKI Solutions and Applications, Secure E-Mail Implementation, and Network Forensics. (Prerequisite: Network Security Fundamentals)

At Roane State Community College (http://ctc.rscc.cc.tn.us/) training as a Computer Security Specialist provides networking professionals the opportunity for career advancement by enhancing their skill set. RSCC describes their target audience as Network Administrators, Network Security Administrators, Firewall and Server Administrators, as well as IT Professionals involved in network support issues. RSCC's first level of certification, the Security Certified Network Professional focuses on the critical areas of security that are the foundational defense of networks: Firewalls and Intrusion Detection Devices. The following overviews provide insight into the contents of each of the courses.

Network Security Fundamentals ... is a 40-hour course in Securing Windows NT/2000, Securing Linux (UNIX),TCP/IP Fundamentals, Advanced TCP/IP, Router Security, Security Fundamentals, Internet Security, General Attack Methods, Specific Attack Methods, Implementing Security

Network Defense and Countermeasures ... is a 40-hour course in Security Fundamentals, Firewalls, Intrusion Detection, Secure Socket Layer, Risk Analysis, Virtual Private Networks, Distributed Denial of Service, Monitoring and Optimizing

RSCC's second certification is an additional 80 hours and is designed for those individuals who wish to take their skills to the next level. The Security Certified Network Architect certification deals extensively with Public Key Infrastructure (PKI) and Biometrics, described as the two most critical areas of network communication. The

program prerequisite is completion of the Network Security Fundamentals and Network Defense and Countermeasures courses, or attaining the SCNP credential. The following overviews provide insight into the contents of each of the courses.

PKI Concepts and Planning ... is a 40-hour course in Cryptography Fundamentals, Strong Authentication, Digital Signatures, PKI Standards, Biometrics Fundamentals, PKI Fundamentals

PKI and Biometrics Implementation ... is a 40-hour course in Sign-on Solutions, PKI Solutions and Applications, Secure E-Mail Implementation, File Encryption Solutions, Certificate Server Deployment, Network Forensics

Conclusion

We identified four distinct approaches to cybersecurity education taken by five American community colleges: Seminole Community College, Northern Virginia Community College, Community College of the Air Force, Edmonds Community College, and Roane State Community College. The specific cybersecurity implementation currently in place at each of these community colleges was profiled. We actively advocate the identification of similar efforts by other two-year colleges, and to that end we have established a website to house basic information on such initiatives. We urge community college faculty and administrators to locate existing cybersecurity implementations at http://www.acmtyc.org and to catalog new initiatives. The community of community colleges certainly can play a vital role in the preparation of professionals for careers related to cybersecurity. Our ongoing efforts are intended to support and promote that important initiative.

U.S. Department of Education
Office of Educational Research and Improvement
(OERI)
National Library of Education (NLE)
Educational Resources Information Center (ERIC)

Reproduction Release
(Specific Document)

I. DOCUMENT IDENTIFICATION:

Title: CYBERSECURITY EDUCATION IN COMMUNITY COLLEGES ACROSS AMERICA	
Author(s): R. CAMPBELL, E. HAWTHORNE	
Corporate Source: ROCK VALLEY COLLEGE	Publication Date: JULY 2002

II. REPRODUCTION RELEASE:

In order to disseminate as widely as possible timely and significant materials of interest to the educational community, documents announced in the monthly abstract journal of the ERIC system, Resources in Education (RIE), are usually made available to users in microfiche, reproduced paper copy, and electronic media, and sold through the ERIC Document Reproduction Service (EDRS). Credit is given to the source of each document, and, if reproduction release is granted, one of the following notices is affixed to the document.

If permission is granted to reproduce and disseminate the identified document, please CHECK ONE of the following three options and sign in the indicated space following.

The sample sticker shown below will be affixed to all Level 1 documents	The sample sticker shown below will be affixed to all Level 2A documents	The sample sticker shown below will be affixed to all Level 2B documents
PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY SAMPLE TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)	PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE, AND IN ELECTRONIC MEDIA FOR ERIC COLLECTION SUBSCRIBERS ONLY, HAS BEEN GRANTED BY SAMPLE TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)	PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE ONLY HAS BEEN GRANTED BY SAMPLE TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
Level 1	Level 2A	Level 2B
☑	☐	☐
Check here for Level 1 release, permitting reproduction and dissemination in microfiche or other ERIC archival media (e.g. electronic) and paper copy.	Check here for Level 2A release, permitting reproduction and dissemination in microfiche and in electronic media for ERIC archival collection subscribers only	Check here for Level 2B release, permitting reproduction and dissemination in microfiche only
Documents will be processed as indicated provided reproduction quality permits. If permission to reproduce is granted, but no box is checked, documents will be processed at Level 1.		

P.002/004
AUG-02-2002 FRI 07:31 AM

I hereby grant to the Educational Resources Information Center (ERIC) nonexclusive permission to reproduce and disseminate this document as indicated above. Reproduction from the ERIC microfiche, or electronic media by persons other than ERIC employees and its system contractors requires permission from the copyright holder. Exception is made for non-profit reproduction by libraries and other service agencies to satisfy information needs of educators in response to discrete inquiries.

Signature:	Printed Name/Position/Title: ROBERT D. CAMPBELL	
Organization/Address: ROCK VALLEY COLLEGE 3301 N. MULFORD RD. ROCKFORD, IL 61114	Telephone: 815-921-4800	Fax: 815-654-5220
	E-mail Address: B.CAMPBELL@RVC.CC.IL.US	Date: 8-2-02

III. DOCUMENT AVAILABILITY INFORMATION (FROM NON-ERIC SOURCE):

If permission to reproduce is not granted to ERIC, or, if you wish ERIC to cite the availability of the document from another source, please provide the following information regarding the availability of the document. (ERIC will not announce a document unless it is publicly available, and a dependable source can be specified. Contributors should also be aware that ERIC selection criteria are significantly more stringent for documents that cannot be made available through EDRS.)

Publisher/Distributor:
Address:
Price:

IV. REFERRAL OF ERIC TO COPYRIGHT/REPRODUCTION RIGHTS HOLDER:

If the right to grant this reproduction release is held by someone other than the addressee, please provide the appropriate name and address:

Name:
Address:

V. WHERE TO SEND THIS FORM:

Send this form to the following ERIC Clearinghouse:

AUG-02-2002 FRI 07:32 AM P.003/004

However, if solicited by the ERIC Facility, or if making an unsolicited contribution to ERIC, return this form (and the document being contributed) to:

ERIC Processing and Reference Facility
4483-A Forbes Boulevard
Lanham, Maryland 20706
Telephone: 301-552-4200
Toll Free: 800-799-3742
e-mail: ericfac@inet.ed.gov
WWW: http://ericfacility.org

EFF-088 (Rev. 2/2001)

AUG-02-2002 FRI 07:32 AM P.004/004